ZARZĄDZENIE NR 10/2020

DYREKTORA CENTRUM INTEGRACJI SPOŁECZNEJ W ŚWIĘTOCHŁOWICACH

z dnia 15 maja 2020 r.

w sprawie Polityki bezpieczeństwa przetwarzania danych osobowych

Na podstawie § 10 ust. 1 Statutu Centrum Integracji Społecznej, stanowiącego załącznik do uchwały nr V/24/11 Rady Miejskiej w Świętochłowicach z dnia 16 lutego 2011 r. w sprawie utworzenia samorządowej jednostki budżetowej o nazwie Centrum Integracji Społecznej w Świętochłowicach (Dz. Urz. Woj. Śl. z 2011 r. nr 82 poz. 1485), w związku z art. 24 ust. 1 i 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), zarządza się, co następuje:

§ 1. W Centrum Integracji Społecznej w Świętochłowicach wprowadza się Politykę bezpieczeństwa przetwarzania danych osobowych, stanowiącą załącznik do zarządzenia.

§ 2. Tracą moc:

1) zarządzenie nr 9/2011 Dyrektora Centrum Integracji Społecznej w Świętochłowicach z dnia 28 czerwca 2011 r. w sprawie określenia polityki bezpieczeństwa i wdrożenia instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
2) zarządzenie nr 6/2018 Dyrektora Centrum Integracji Społecznej w Świętochłowicach z dnia 21 września 2018 r. w sprawie wprowadzenia/zmiany Polityki Bezpieczeństwa Danych Osobowych w Centrum Integracji Społecznej w Świętochłowicach.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

Mirosław Karwot
Inspektor Ochrony Danych

Dyrektor
Centrum Integracji Społecznej
w Świętochłowicach
Magdalena Domańska-Rosin

SPRAWDZONO P/W
FORMALNOPRAWNYM
Sławomir Czyż
Radca Prawny

Załącznik do zarządzenia
nr 10/2020 Dyrektora Centrum
Integracji Społecznej
w Świętochłowicach z dnia
15 maja 2020 r.

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

Rozdział 1

Postanowienia ogólne

§ 1. Polityka bezpieczeństwa zwana dalej „Polityką", określa środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych oraz sposób przepływu danych pomiędzy poszczególnymi systemami. Zawiera wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, a także tryb postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych w systemach informatycznych lub kartotekach albo w sytuacji zaistnienia podejrzenia o powstaniu takiego naruszenia.

§ 2. Szczegółowe zestawienie przetwarzanych zbiorów osobowych wraz z ich charakterystyką i zawartością merytoryczną, a także opisem pól informacyjnych i wzajemnych zależności występujących pomiędzy poszczególnymi zbiorami, sporządza Administrator zgodnie ze wzorem, stanowiącym załącznik nr 17.

§ 3. Obszar fizyczny przetwarzania danych określa szczegółowo Administrator zgodnie ze wzorem, stanowiącym załącznik nr 9.

§ 4. Zbiory osobowe przetwarzane są z wykorzystaniem:

1) systemu informatycznego oraz informacji udostępnianych z jego wykorzystaniem;
2) informacji zgromadzonych i przetwarzanych w formie tradycyjnej.

§ 5. Dostęp do Internetu realizowany jest poprzez stałe łącze.

§ 6. Każde naruszenie zasad Polityki może być uznane za poważne naruszenie podstawowych obowiązków pracowniczych lub wynikających z umów cywilnych o współpracy i może skutkować konsekwencjami, zgodnie z Kodeksem pracy lub

odpowiednimi przepisami regulującymi zasady współpracy, jak również odpowiedzialnością przewidzianą w ustawie o ochronie danych osobowych.

Rozdział 2

Cel powstania dokumentu

§ 7. Celem powstania niniejszej Polityki jest realizacja obowiązków wynikających z przepisów dotyczących ochrony danych osobowych, jak również spełnienie wymagań chroniących prywatność i godność osób, których dane osobowe są przetwarzane przez Administratora Danych.

§ 8. Przedmiotem Polityki jest określenie, opisanie i zawarcie w tym i załączonych dokumentach, zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych osobowych objętych ochroną, a w szczególności zabezpieczeń danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Rozdział 3

Podstawa prawna oraz zakres obowiązywania

§ 9. Polityka została przygotowana, aby spełnić wymogi:

1) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) zwane dalej RODO.
2) ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2019 poz. 1781).

§ 10. Polityka obowiązuje przy przetwarzaniu wszelkich danych osobowych w Centrum Integracji Społecznych w Świętochłowicach.

§ 11. Sposób postępowania przy przetwarzaniu danych opisany jest w osobnych procedurach i instrukcjach.

§ 12. Podmioty zewnętrzne, które będą przetwarzać dane osobowe na zlecenie Administratora Danych, zobowiązane są opracować własną dokumentację i zabezpieczyć przetwarzane dane osobowe zgodnie z wymogami prawa. Powierzenie danych powinno odbywać się na podstawie umowy powierzenia przetwarzania danych, której wzór stanowi

załącznik nr 14. Wzór wykazu podmiotów, z którymi zostały podpisane umowy powierzenia przetwarzania danych stanowi załącznik nr 15.

§ 13. W przypadku, kiedy nie zachodzi proces powierzenia przetwarzania danych osobowych, ale istnieje prawdopodobieństwo dostępu do danych należy podpisać z podmiotem, który może taki dostęp posiadać Klauzulę poufności, której wzór stanowi załącznik nr 25.

Rozdział 4

Definicje

§ 14. Użyte w polityce określenia oznaczają:

1) dane osobowe - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
2) przetwarzanie - operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
3) ograniczenie przetwarzania - oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
4) profilowanie - dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
5) pseudonimizacja - przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych

informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

6) zbiór danych - uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

7) administrator - osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

8) podmiot przetwarzający - osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

9) odbiorca - osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

10) strona trzecia - osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;

11) zgoda osoby, której dane dotyczą - dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

12) naruszenie ochrony danych osobowych - naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

13) dane genetyczne - dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;

14) dane biometryczne - dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;

15) dane dotyczące zdrowia - dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;

16) główna jednostka organizacyjna:

   a) jeżeli chodzi o administratora posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim – miejsce, w którym znajduje się jego centralna administracja w Unii, a jeżeli decyzje co do celów i sposobów przetwarzania danych osobowych zapadają w innej jednostce organizacyjnej tego administratora w Unii i ta jednostka organizacyjna ma prawo nakazać wykonanie takich decyzji, to za główną jednostkę organizacyjną uznaje się jednostkę organizacyjną, w której zapadają takie decyzje,

   b) jeżeli chodzi o podmiot przetwarzający posiadający jednostki organizacyjne w więcej niż jednym państwie członkowskim – miejsce, w którym znajduje się jego centralna administracja w Unii lub, w przypadku gdy podmiot przetwarzający nie ma centralnej administracji w Unii – jednostkę organizacyjną podmiotu przetwarzającego w Unii, w której odbywają się główne czynności przetwarzania w ramach działalności jednostki organizacyjnej podmiotu przetwarzającego, w zakresie w jakim podmiot przetwarzający podlega szczególnym obowiązkom na mocy RODO;

17) przedstawiciel - osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii, która została wyznaczona na piśmie przez administratora lub podmiot przetwarzający na mocy art. 27 do reprezentowania administratora lub podmiotu przetwarzającego w zakresie ich obowiązków wynikających z RODO;

18) przedsiębiorca - osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą;

19) grupa przedsiębiorstw - przedsiębiorstwo sprawujące kontrolę oraz przedsiębiorstwa przez nie kontrolowane;

20) wiążące reguły korporacyjne - polityki ochrony danych osobowych stosowane przez administratora lub podmiot przetwarzający, którzy posiadają jednostkę organizacyjną na terytorium państwa członkowskiego, przy jednorazowym lub wielokrotnym przekazaniu danych osobowych administratorowi lub podmiotowi przetwarzającemu w co najmniej jednym państwie trzecim w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą;

21. organ nadzorczy - niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51;

22. organ nadzorczy, którego sprawa dotyczy - organ nadzorczy, którego dotyczy przetwarzanie danych osobowych, ponieważ:
    a) administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną na terytorium państwa członkowskiego tego organu nadzorczego,
    b) przetwarzanie znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, mające miejsce zamieszkania w państwie członkowskim tego organu nadzorczego lub
    c) wniesiono do niego skargę;

23) transgraniczne przetwarzanie:
    a) przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności jednostek organizacyjnych w więcej, niż jednym państwie członkowskim administratora lub podmiotu przetwarzającego w Unii posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim albo
    b) przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego w Unii, ale które znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim;

24) mający znaczenie dla sprawy i uzasadniony sprzeciw - sprzeciw wobec projektu decyzji dotyczącej tego, czy doszło do naruszenia RODO lub czy planowane działanie wobec administratora lub podmiotu przetwarzającego jest zgodne z RODO, który to sprzeciw

musi jasno wskazywać wagę wynikającego z projektu decyzji ryzyka naruszenia podstawowych praw lub wolności osób, których dane dotyczą, oraz gdy ma to zastosowanie – wagę ryzyka zakłócenia swobodnego przepływu danych osobowych w Unii;

25) usługa społeczeństwa informacyjnego oznacza usługę w rozumieniu art. 1 ust. 1 lit. b) dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/1535 (1);

26. organizacja międzynarodowa - organizację i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy.

Rozdział 5

Sposób przechowywania, udostępniania i modyfikacji polityki

§ 15. Polityka została zatwierdzona w Centrum Integracji Społecznych w Świętochłowicach w dniu 01.10.2018 jako dokument obowiązujący.

§ 16. Niniejszy dokument powinien być regularnie przeglądany i aktualizowany przez Inspektora Ochrony Danych lub przez Administratora Danych.

§ 17. 1. Zmiany w dokumencie Polityki oraz załącznikach wprowadzane są w chwili pojawienia się ważnych okoliczności lub nowego przepisu, istotnego dla spójności i aktualności Polityki, bądź aktualizacji dotychczasowych przepisów dotyczących ochrony lub przetwarzania danych osobowych. Zmiany zatwierdzane są przez Administratora Danych.

2. Informacje o zmianach podawane są do wiadomości osób uczestniczących w przetwarzaniu danych osobowych poprzez publikację w intranecie lub dokumentach formalnych udostępnianych w ustalony wewnętrznie sposób.

3. W przypadku zatwierdzenia nowej wersji Polityki jest ona drukowana, a wydruk dołączany jest do prowadzonej dokumentacji ochrony danych osobowych. Załączniki mogą być przechowywane w formie elektronicznej. Ich wydruk może być wykonywany w razie zaistnienia takiej konieczności, na zlecenie Administratora Danych lub Inspektora Ochrony Danych.

§ 18. Dokument Polityki, wraz z załącznikami, stanowi tajemnicę Centrum Integracji Społecznej w Świętochłowicach i jest klasyfikowany jako dokument wewnętrzny.

Rozdział 6

Podstawowe zasady przetwarzania danych osobowych

§ 19. 1. Dane osobowe muszą być:

1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość");
2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu");
3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych");
4) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość");
5) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy RODO w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania");
6) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

2. Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność").

Rozdział 7

Przetwarzanie szczególnych kategorii danych osobowych

§ 20. 1. Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

2. Ust. 1 nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków:

1) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1;
2) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;
3) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
4) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;
5) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
6) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;

7) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;

8) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3;

9) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;

10) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

3. Dane osobowe, o których mowa w ust. 1, mogą być przetwarzane do celów, o których mowa w ust. 2 pkt 8, jeżeli są przetwarzane przez – lub na odpowiedzialność – pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe lub przez inną osobę również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe.

4. Państwa członkowskie mogą zachować lub wprowadzić dalsze warunki, w tym ograniczenia w odniesieniu do przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia.

Rozdział 8

Przetwarzanie danych osobowych dotyczących wyroków skazujących i naruszeń prawa

§ 21. Przetwarzania danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa na podstawie art. 6 ust. 1 RODO wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. Wszelkie kompletne rejestry wyroków skazujących są prowadzone wyłącznie pod nadzorem władz publicznych.

Rozdział 9

Zgodność przetwarzania z prawem

§ 18. 1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

1) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
2) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
3) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
4) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
5) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
6) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

2. Akapit pierwszy pkt 6 nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

Rozdział 10

Zasady przetwarzania danych

§ 22. 1. Przetwarzanie danych osobowych z użyciem sprzętu komputerowego oraz kartotek odbywa się wyłącznie na obszarze wyznaczonym przez Administratora Danych.

2. Obszar pomieszczeń Centrum Integracji Społecznej w Świętochłowicach w którym przetwarzane są dane osobowe, obejmuje zarówno miejsca, w których wykonuje się operacje na danych osobowych (wpisuje, modyfikuje, kopiuje), jak również miejsca, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych, stacje komputerowe i inne urządzenia komputerowe).

3. Obszar przetwarzania danych osobowych zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych.

4. Pomieszczenia stanowiące obszar przetwarzania danych powinny być zamykane na klucz. Przed opuszczeniem pomieszczeń należy zamknąć okna, a także usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach.

5. Szczegółowy wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe określa dokument, którego wzór stanowi załącznik nr 9 do Polityki.

6. Wzór Wykazu kont i aplikacji przetwarzających dane osobowe stanowi załącznik nr 4.

§ 23. 1. Szczegółowe zestawienie przetwarzanych zbiorów wraz z ich charakterystyką i opisem struktury sporządza Administrator zgodnie ze wzorem, stanowiącym załącznik nr 17.

2. Centrum Integracji Społecznej w Świętochłowicach korzysta z oprogramowania Firmy Vulcan Pakiet Finanse Optivum, Płace Optivum, Kadry Optivum, Kasa Optivum, Inwentarz Optivum, Płatnik, FillUp.

3. Oprogramowanie wspiera w procesach: kadrowych, księgowych, płacowych.

4. W Centrum Integracji Społecznej w Świętochłowicach utworzono i wydzielono następujące zbiory danych osobowych:

1) kadry – zbiór pracowników, zbiór płac pracowników, zbiór uczestników CIS, zbiór płac uczestników CIS, zbiór osób współpracujących z Centrum Integracji Społecznej w oparciu o umowy cywilnoprawne;

2) księgowość – zbiór pracowników, zbiór płac pracowników, zbiór uczestników CIS, zbiór płac uczestników CIS, zbiór osób współpracujących z Centrum Integracji Społecznej w oparciu o umowy cywilnoprawne, zbiór kontrahentów;
3) dane uczestników CIS – zbiór uczestników CIS; zbiór płac uczestników CIS;
4) dokumentacja CIS (obieg dokumentów) - zbiór pracowników, zbiór uczestników CIS, zbiór płac uczestników CIS, zbiór osób współpracujących z Centrum Integracji Społecznej w oparciu o umowy cywilnoprawne, zbiór kontrahentów;
5) składnica akt kadry - zbiór pracowników, zbiór płac pracowników, zbiór uczestników CIS, zbiór płac uczestników CIS, zbiór osób współpracujących z Centrum Integracji Społecznej w oparciu o umowy cywilnoprawne;
6) składnica akt księgowość - zbiór uczestników CIS, zbiór płac uczestników CIS, zbiór osób współpracujących z Centrum Integracji Społecznej w oparciu o umowy cywilnoprawne, zbiór kontrahentów, zbiór płac pracowników, zbiór pracowników;
7) składnica akt uczestnicy CIS - zbiór pracowników, zbiór płac pracowników, zbiór uczestników CIS, zbiór płac uczestników CIS, zbiór osób współpracujących z Centrum Integracji Społecznej w oparciu o umowy cywilnoprawne;
8) składnica akt - dokumenty dot. projektów dofinansowanych z źródeł zewnętrznych – zbiór uczestników CIS, zbiór płac uczestników CIS;
9) dane dotyczące monitoringu - dane wizerunkowe, sposób zachowania się osób przebywających na terenie obiektu, numery rejestracyjne samochodów, kolor i marka pojazdu.

§ 18. Przepływ informacji pomiędzy zbiorami danych a systemem informatycznym jest dwukierunkowy (do odczytu i do zapisu).

Rozdział 11

Warunki wyrażenia zgody

§ 24. 1. Jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.

2. Jeżeli osoba, której dane dotyczą, wyrażą zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie RODO nie jest wiążąca.

3. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.

4. Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.

5. Wzór zgody na przetwarzanie danych osobowych osoby dorosłej stanowi załącznik nr 7.

6. Wzór zgody na przetwarzanie danych osobowych dziecka/podopiecznego stanowi załącznik nr 23.

7. Wzór zgody na upublicznienie wizerunku osoby dorosłej stanowi załącznik nr 10.

8. Wzór zgody na upublicznienie wizerunku dziecka/podopiecznego stanowi załącznik nr 22.

Rozdział 12

Odpowiedzialność za bezpieczeństwo danych osobowych, obowiązki Administratora Danych oraz Inspektora Danych Osobowych

§ 25. 1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:

1) pseudonimizację i szyfrowanie danych osobowych;
2) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

3) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
4) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

2. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

3. Wywiązywanie się z obowiązków, o których mowa w ust. 1, można wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42.

4. Administrator oraz podmiot przetwarzający podejmują działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego.

5. Wytyczne w zakresie Oceny ryzyka zostały przedstawione w załączniku nr 3.

§ 26. Obowiązki Administratora Danych:

1) uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane;
2) jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych;
3) stosowanie zatwierdzonych kodeksów postępowania, o których mowa w art. 40 RODO, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42 RODO, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.

§ 27. Zadania Inspektora Ochrony Danych:

1) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
2) monitorowanie przestrzegania rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
3) udzielanie na żądanie zaleceń, co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
4) współpraca z organem nadzorczym;
5) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;
6) Inspektor Ochrony Danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania;
7) wzór dokumentu zawierającego Wykaz kontroli stanowi załącznik nr 18;
8) wzór dokumentu zawierającego Sprawozdanie ze sprawdzenia zgodności przetwarzania danych z przepisami ODO stanowi załącznik nr 6.

Rozdział 13

Wymogi i informacje dotyczące ochrony i przetwarzania danych osobowych

§ 18. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są w Centrum Integracji Społecznej w Świętochłowicach dane osobowe sporządza się zgodnie ze wzorem, stanowiącym załącznik nr 9.

2. Wykaz zbiorów danych osobowych wraz z bazami danych w których przetwarzane są dane osobowe sporządza się zgodnie ze wzorem, stanowiącym załącznik nr 17.

3. Pracownicy wykonujący operacje przetwarzania danych osobowych muszą posiadać upoważnienie do przetwarzania danych osobowych wydane przez Administratora danych. Wzór upoważnienia stanowi załącznik nr 16.

4. Pracownik posiadający upoważnienie do przetwarzania danych musi zostać wpisany do Rejestru osób upoważnionych do przetwarzania danych osobowych, który jest prowadzony przez Administratora danych. Wzór Rejestru osób upoważnionych do przetwarzania danych osobowych stanowi załącznik nr 24.

5. Zgodnie z art. 30 RODO Administrator powinien prowadzić Rejestr czynności przetwarzania. Rejestr może być prowadzony w formie elektronicznej. Wzór Elektronicznego rejestru czynności przetwarzania stanowi załącznik nr 2.

§ 28. 1. Osoba fizyczna, której dane są przetwarzane przez Administratora danych, może się zwrócić do niego z wnioskiem o udostępnienie danych osobowych. Wzór wniosku stanowi załącznik nr 13.

2. Każde udostępnienie danych należy odnotować. W przypadku udostępnienia danych osobie, której dane dotyczą wzór Wykazu stanowi załącznik nr 12. W przypadku udostępnienia danych innym podmiotom wzór Wykazu stanowi załącznik nr 11.

Rozdział 14

Postępowanie w przypadkach stwierdzenia naruszenia ochrony danych osobowych

§ 29. 1. W przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55 RODO, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

2. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.

3. Szczegółowa Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych stanowi załącznik nr 21.

4. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:

1) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
2) zawierać imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
3) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;

4) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

5. W zakresie, w jakim informacji nie da się udzielić w czasie ustalonym w ust. 1, można je udzielać sukcesywnie bez zbędnej zwłoki

6. Wzór Zgłoszenia naruszenia ochrony danych osobowych do organu nadzorczego stanowi załącznik nr 5.

§ 30. 1. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu na zweryfikowanie przestrzegania niniejszego artykułu.

2. Wzór Rejestru incydentów naruszenia ochrony danych osobowych stanowi załącznik nr 8.

Rozdział 15

Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

§ 31. 1. Administrator Danych wdraża odpowiednie środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

2. Zalecenia dotyczące możliwych do zastosowania środków określa załącznik nr 20.

Rozdział 16

Zmiany i udostępnianie tekstu polityki

§ 32. Dopuszcza się dokonywanie zmian w niniejszym dokumencie oraz dokumentach powiązanych tylko przez osoby upoważnione, na zasadach opisanych w rozdziale 5 Polityki.

§ 33. Tekst niniejszej Polityki wraz z załącznikami zostanie udostępniony osobom przetwarzającym dane, aby mogły się one z nim zapoznać i postępować zgodnie z jej postanowieniami.

Rozdział 17

Znajomość polityki

§ 34. 1. Do zapoznania się z niniejszym dokumentem Polityki oraz stosowania zawartych w niej zasad zobowiązane są wszystkie osoby przetwarzające dane osobowe w zbiorze danych osobowych administrowanym przez Administratora danych.

2. Po zapoznaniu z zasadami przetwarzania danych osobowych osoby przetwarzające dane osobowe podpisują odpowiednie Oświadczenie, które stanowi załącznik nr 19.

Rozdział 18

Pozostałe informacje dotyczące systemów informatycznych i baz danych

§ 35. Pozostałe informacje dotyczące systemów informatycznych i baz danych są zawarte w „Instrukcji zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych", która stanowi załącznik nr 1 do niniejszej Polityki.

Załączniki do Polityki
bezpieczeństwa przetwarzania
danych osobowych

Załącznik nr 1

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI SŁUŻĄCYMI DO PRZETWARZANIA DANYCH OSOBOWYCH

Rozdział 1

Postanowienia ogólne

§ 1. Niniejsza instrukcja stanowi podstawę do określenia sposobu zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Centrum Integracji Społecznej w Świętochłowicach.

§ 2. Inspektor Ochrony Danych lub Administrator Danych odpowiada za weryfikację niniejszej instrukcji w przypadku uzasadnionych zmian w przepisach prawnych dotyczących przetwarzania danych osobowych w systemach informatycznych, jak również zmian organizacyjno-funkcjonalnych zachodzących w Centrum Integracji Społecznej w Świętochłowicach.

§ 3. Przetwarzanie danych w systemie informatycznym może być realizowane wyłącznie poprzez dopuszczone do eksploatacji licencjonowane oprogramowanie.

§ 4. 1. Administratorem Danych jest Dyrektor Centrum Integracji Społecznej w Świętochłowicach.

2. Administrator danych powierza obsługę techniczną i konserwację urządzeń komputerowych zewnętrznemu podmiotowi, zwanemu dalej Administratorem Systemu Informatycznego, na podstawie umowy powierzenia przetwarzania danych osobowych.

§ 5. 1. Dostęp do baz danych oraz systemów informatycznych przetwarzających dane osobowe mają wyłącznie osoby posiadające stosowne upoważnienia wydane przez Administratora Danych zgodnie z załącznikiem nr 16.

2. Prowadzony jest rejestr osób upoważnionych do przetwarzania danych osobowych.

3. Każda upoważniona osoba („Operator danych") przed przystąpieniem do pracy przy przetwarzaniu danych osobowych zobowiązana jest zapoznać się z:

1) postanowieniami Ustawy o Ochronie Danych Osobowych;
2) Polityką Bezpieczeństwa przetwarzania danych osobowych w Centrum Integracji Społecznej w Świętochłowicach;

3) obowiązującą w Centrum Integracji Społecznej w Świętochłowicach Instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych – załącznik nr 21 do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych;

4) niniejszą instrukcją.

4. Fakt zapoznania się z przepisami, o których mowa w ust. 3, operator danych zobowiązany jest potwierdzić własnoręcznym podpisem we właściwym dokumencie, przedstawionym mu do podpisania przez Administratora Danych – załącznik nr 19 do Polityki Bezpieczeństwa.

5. Uprawnienia do przetwarzania danych osobowych odbierane są trwale w przypadku ustania stosunku pracy.

6. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia nawet w przypadku ustania stosunku pracy.

7. Teksty wszystkich wymienionych dokumentów i aktów prawnych znajdują się do wglądu w siedzibie firmy.

Rozdział 2

Obszar przetwarzania danych

§ 6. Dane osobowe przetwarzane są przez Administratora Danych w następujących budynkach, pomieszczeniach, tworzących obszar przetwarzania danych osobowych: Centrum Integracji Społecznej w Świętochłowicach, ul Sądowa 1, 41-605 Świętochłowice.

§ 4. 1. Dostęp do pomieszczeń, w których przetwarzane są dane osobowe zawarte w zbiorach administrowanych przez Administratora Danych mają: pracownicy i współpracownicy Administratora Danych posiadający odpowiednie upoważnienie, uprawnione przez Administratora Danych oraz (na mocy umowy powierzenia przetwarzania danych) przez Procesora osoby i pracownicy firm współpracujących. Przebywanie w tych pomieszczeniach osób niedopuszczonych/nieupoważnionych do przetwarzania danych osobowych może się odbywać tylko w obecności przedstawiciela Administratora Danych, lub przedstawiciela Procesora lub osób upoważnionych.

2. W przypadku opuszczenia pomieszczeń (wchodzących w skład obszaru przetwarzania danych osobowych) przez osoby upoważnione, pomieszczenia te zobowiązane są opuścić również osoby nieupoważnione, znajdujące się w tym czasie pod ich nadzorem.

3. W celu ograniczenia dostępu osób postronnych do pomieszczeń, w których zlokalizowano przetwarzanie danych osobowych, pod nieobecność upoważnionych pracowników Centrum Integracji Społecznej w Świętochłowicach należy zastosować poniższe środki:

1) drzwi wejściowe powinny być zabezpieczone odpowiednimi zamkami;
2) pomieszczenia, w których zlokalizowano przetwarzanie danych osobowych powinny być wyposażone w zamykane szafy oraz inne meble z zamykanymi segmentami;
3) klucze zapasowe do pomieszczeń powinny być przechowywane w specjalnej szafie i powinny być wydawane w sytuacjach awaryjnych;
4) ochrona obiektu Centrum Integracji Społecznej w Świętochłowicach powinna być zapewniona przez cały rok;
5) dokumenty powinny być przechowywane w przeznaczonych do tego celu zamkniętych szafach, do których dostęp powinni mieć wyłącznie upoważnieni pracownicy Centrum Integracji Społecznej w Świętochłowicach;
6) użytkownicy odpowiedzialni są za rzetelne prowadzenie kartotek, ich kompletność oraz ochronę i zabezpieczenie po godzinach pracy;
7) każdy nowo zatrudniony pracownik przed uzyskaniem dostępu do danych osobowych podlega przeszkoleniu w zakresie przepisów o ochronie danych osobowych oraz wynikających z nich zadań oraz obowiązków;
8) wszyscy użytkownicy podlegają okresowym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym (wymiana sprzętu na nowszej generacji, zmiana oprogramowania) oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmian wewnętrznych regulacji;
9) użytkownicy powinni mieć świadomość możliwości zaistnienia sytuacji naruszenia ochrony danych osobowych.

§ 4. W przypadku utraty klucza osoba upoważniona zobowiązana jest do natychmiastowego poinformowania o tym fakcie Administratora Danych.

§ 7. 1. W przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych, lub podejrzenia takiego naruszenia, każda osoba posiadająca taką wiedzę zobowiązana jest poinformować o tym fakcie Administratora Danych lub Inspektora Ochrony Danych.

2. Do przesłanek wskazujących na naruszenie bezpieczeństwa ochrony danych należą m. in.:

1) próby błędnych logowań do systemów przetwarzających dane osobowe;

2) próby nieautoryzowanego dostępu do baz danych;
3) próby wynoszenia danych na nośnikach pamięci masowych;
4) pozostawienie wydruków danych osobowych na drukarkach, kserokopiarkach lub innych urządzeniach poligraficznych lub w miejscach niechronionych,
5) wysyłanie, przez osoby nieupoważnione, dokumentów lub informacji zawierających dane osobowe za pośrednictwem poczty elektronicznej lub konwencjonalnej oraz urządzeń teletransmisyjnych,

§ 8. Pracowników Centrum Integracji Społecznej w Świętochłowicach obowiązuje bezwzględny zakaz wynoszenia płyt lub innych nośników z oprogramowaniem lub innymi danymi, będącymi własnością Centrum Integracji Społecznej w Świętochłowicach poza teren siedziby chyba, że zgodę na tę czynność wyrazi Administrator Danych.

§ 9. Pracownikom Centrum Integracji Społecznej w Świętochłowicach wolno używać powierzonego sprzętu jedynie w celach służbowych. Administrator Danych może przeprowadzić kontrolę komputera, poczty elektronicznej oraz wykorzystania Internetu bez wiedzy pracowników.

§ 10. Urządzenia, dyski lub inne nośniki informacji przeznaczone do:
1) likwidacji – powinny być pozbawione danych poprzez formatowanie oraz fizyczne uszkodzenie uniemożliwiające ich odczytanie, z wykonanych czynności należy sporządzić protokół zniszczenia;
2) przekazania – powinny być pozbawione zapisu zawierającego dane osobowe, z wykonanych czynności należy sporządzić protokół przekazania;
3) naprawy – powinny być pozbawione zapisu danych osobowych lub naprawiane pod nadzorem osoby upoważnionej, z wykonanych czynności należy sporządzić protokół naprawy.

§ 11. Wydruki zawierające dane osobowe przeznaczone do usunięcia powinny być niszczone w niszczarce, natomiast inne wydruki powinny być przechowywane w warunkach uniemożliwiających dostęp do nich osób nieupoważnionych.

§ 12. 1. Na stanowiskach pracy, na których przetwarzane są dane osobowe, ekrany monitorów powinny być ustawione w sposób uniemożliwiający osobom trzecim wgląd w wyświetlane informacje.

2. W razie przerwania pracy stosuje się „wygaszacz ekranu" i blokowanie komputera hasłem.

3. Każdy z komputerów powinien być zabezpieczony hasłem dostępu.

§ 13. W przypadku wystąpienia zagrożenia (zdarzenie losowe – ogień, huragan, woda) powodującego konieczność przeprowadzenia ewakuacji osób lub mienia z pomieszczeń, w których przetwarzane są dane osobowe, należy niezwłocznie powiadomić o tym fakcie Administratora Danych oraz Inspektora Ochrony Danych , a następnie w miarę możliwości przerwać pracę, zamknąć system informatyczny, zabezpieczyć dane osobowe gromadzone w kartotekach tradycyjnych. Osoby biorące udział w akcji ratunkowej, mają prawo wejść do pomieszczeń, w których przetwarzane są dane osobowe.

Rozdział 3

Procedura przydziału i zmiany hasel oraz rejestracji i wyrejestrowania operatorów danych w systemach informatycznych, w których przetwarzane są dane osobowe; stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

§ 14. Warunkiem uzyskania dostępu do systemów jest posiadanie przez użytkownika systemu własnego identyfikatora i hasła do aplikacji, a w przypadku Administratorów Systemów Informatycznych dodatkowo dedykowanego klucza ssh lub certyfikatu niezbędnego do komunikacji z serwerami i/lub aplikacjami.

§ 15. Wprowadzona zostaje hierarchia użytkowników (operatorów danych) związana z uprawnieniami jakie posiadają. Użytkownicy pełniący funkcje administracyjne mają szerszy zakres uprawnień niż użytkownicy tych funkcji nie pełniący. Administrator Danych, przyznając upoważnienia do przetwarzania danych osobowych, stosuje zasadę przyznawania uprawnień w minimalnym zakresie, niezbędnym do wykonania czynności służbowych przez danego użytkownika

§ 16. 1. Identyfikatory, hasła lub inne mechanizmy uwierzytelniające użytkownika przydzielane są przez Administratora Danych lub Administratorów Systemów Informatycznych (za zgodą Administratora Danych) na wniosek zainteresowanego potwierdzony przez upoważnioną przez Administratora Danych oraz osobę o uprawnieniach kierowniczych sprawującą nadzór nad pracownikiem, współpracownikiem lub zleceniobiorcą.

2. Administrator Danych ewidencjonuje identyfikatory użytkowników mających uprawnienia dostępu do systemów związanych z przetwarzaniem danych osobowych.

3. Każda osoba posiada własny identyfikator (lub identyfikatory w przypadku braku możliwości korzystania z tego samego identyfikatora w różnych systemach) i ma ściśle określony zakres praw dostępu do zasobów systemów informatycznych w których przetwarzane są dane osobowe

4. Do identyfikatora, uprawniającego do korzystania z systemu operacyjnego komputera lub serwera, przypisane są prawa dostępu do zasobów z których korzysta przetwarzając dane osobowe.

5. Identyfikator użytkownika może zostać aktywowany tylko osobie, która zapoznała się przepisami dotyczącymi ochrony danych osobowych zawartymi w Ustawie oraz Rozporządzeniach wykonawczych, obowiązującymi w Centrum Integracji Społecznej w Świętochłowicach, politykami, instrukcjami i procedurami w zakresie przetwarzania danych osobowych oraz która podpisała zobowiązania poufności przetwarzania danych oraz stosowanych zabezpieczeń i zobowiązała się do ponoszenia odpowiedzialności z tego tytułu.

§ 13. 1. Stosowane są następujące rodzaje haseł:

1) hasła startowe do BIOS komputera, na którym przetwarzane są dane osobowe;
2) hasła logowania do systemu operacyjnego komputera lub serwera, na którym przetwarzane są dane osobowe;
3) hasła do wygaszacza ekranu, o ile jest dostępny;
4) hasła dostępu do systemów informatycznych lub aplikacji służących do przetwarzania danych osobowych;
5) hasła dostępu do baz danych.

2. O ile to możliwe, wszystkie hasła, o których mowa w ust. 1, powinny być różne.

§ 17. Zasady postępowania z hasłami użytkowników (operatorów danych):

1) hasła użytkowników (operatorów danych) muszą się składać z co najmniej 8 znaków i muszą zawierać duże i małe litery, cyfry oraz znaki specjalne. Powinny być zmieniane co 30 dni (kategoria D – systemy przetwarzające dane osobowe);
2) hasła nie powinny zawierać imion, nazwisk, nazw własnych ani żadnych innych popularnych lub możliwych do odgadnięcia słów;
3) haseł nie wolno udostępniać ani dopuścić do ich ujawnienia;
4) w sytuacji możliwego naruszenia bezpieczeństwa danych osobowych lub podejrzenia ujawnienia hasła obowiązuje konieczność niezwłocznej zmiany wszystkich stosowanych przez użytkownika haseł;
5) zarówno obecne, jak i wszystkie nieaktualne hasła objęte są ścisłą tajemnicą.

§ 18. Hasła Administratorów do systemów i serwerów powinny spełniać wymagania wynikające z wewnętrznych polityk Procesora. Zalecane jest aby przynajmniej:

1) hasła Administratorów oraz systemowe składały z co najmniej 14 znaków i zawierały duże i małe litery, cyfry oraz znaki specjalne. Powinny być zmieniane co 30 dni (kategoria A – systemy i serwery o znaczeniu strategicznym);
2) hasła nie mogą zawierać imion, nazwisk, nazw własnych ani żadnych innych popularnych lub możliwych do odgadnięcia słów;
3) nie wolno udostępniać ani dopuścić do ujawnienia hasła;
4) zarówno obecne, jak i wszystkie nieaktualne hasła objęte są ścisłą tajemnicą;
5) hasła dostępu do baz danych oraz hasła administracyjne do serwerów i aplikacji wewnętrznych systemów informatycznych przetwarzających dane osobowe należy zmieniać co 30 dni, o ile nie ma ważnych przeciwskazań natury technologicznej. Hasła do pozostałych systemów powinny być zmieniane nie rzadziej niż co 3 miesiące. Dodatkowo obowiązuje zmiana wszystkich haseł administracyjnych każdorazowo w sytuacji stwierdzenia możliwego naruszenia bezpieczeństwa systemów informatycznych lub danych osobowych, podejrzenia ujawnienia któregoś z haseł lub odejścia z zespołu Administratora;
6) kopie aktualnych haseł administracyjnych (do kont, serwerów, systemów, aplikacji oraz baz danych) powinny być deponowane w zaklejonej kopercie/kopertach w bezpiecznym, niedostępnym dla osób nieuprawnionym miejscu.

§ 19. W przypadku cofnięcia operatorowi danych prawa do przetwarzania danych osobowych (np. w związku ze zmianą zakresu obowiązków lub stanowiska, rozwiązaniem umowy o pracę lub zakończeniem współpracy) obowiązują następujące zasady:

1) zobowiązania do nierozpowszechniania i niewykorzystywania poufnych informacji zdobytych w trakcie wykonywania powierzonych prac zachowują ważność także po cofnięciu uprawnień;
2) operator musi zwrócić wszelkie dokumenty i inne materiały dotyczące zbiorów i baz danych osobowych, przetwarzanych danych osobowych lub stosowanych zabezpieczeń;
3) z chwilą cofnięcia uprawnienia do przetwarzania danych osobowych wszystkie identyfikatory wykorzystywane przez operatora danych zostają, we współpracy z Administratorem Danych, zablokowane i wyrejestrowane z systemów, a wszystkie hasła z nimi powiązane tracą ważność;

4) identyfikatory są przechowywane i nie są przydzielane żadnemu innemu operatorowi danych.

Rozdział 4

Procedury rozpoczęcia, zakończenia pracy i obsługi komputera

§ 20. 1. Każdorazowo przy rozpoczęciu pracy operatorzy danych mają obowiązek podać hasło startowe komputera, a następnie zalogować się do systemu informatycznego (system operacyjny lub aplikacja) w którym przetwarzane są dane osobowe.

2. Operator danych rozpoczynając pracę zobowiązany jest dopilnować, czy zostało uruchomione oprogramowanie antywirusowe monitorujące komputer, jeśli takowe jest dostępne.

3. Wszelkie zauważone okoliczności wskazujące na możliwość naruszenia bezpieczeństwa danych osobowych muszą zostać bezzwłocznie zgłoszone do Administratora Danych.

§ 21. 1. Jeśli istnieje taka możliwość, to muszą być stosowane wygaszacze ekranu zabezpieczone hasłem. Wygaszacz powinien się włączyć automatycznie po maks. 10 minutach bezczynności, dodatkowo operator danych powinien mieć możliwość ręcznego włączenia wygaszacza, do czego jest również zobowiązany przy opuszczaniu stanowiska pracy przy komputerze.

2. Wyłączenie wygaszacza ekranu wymaga podania hasła operatora danych lub administratora komputera na którym wygaszacz został uruchomiony.

§ 22. 1. Po zakończeniu pracy operator danych oraz administrator jest zobowiązany wylogować się z aplikacji/systemu oraz zabezpieczyć komputer przed dostępem do danych przez osoby nieuprawnione.

2. W uzasadnionych przypadkach administratorzy mogą uzyskać od Administratora Danych lub Administratora Systemu Informatycznego zgodę na odstępstwa od zasad opisanych w punkcie poprzedzającym, w zakresie konieczności wylogowywania się z aplikacji lub systemów.

Rozdział 5

Komputery przenośne wykorzystywane do przetwarzania danych osobowych

§ 18. Hasła Administratorów do systemów i serwerów powinny spełniać wymagania wynikające z wewnętrznych polityk Procesora. Zalecane jest aby przynajmniej:

1) hasła Administratorów oraz systemowe składały z co najmniej 14 znaków i zawierały duże i małe litery, cyfry oraz znaki specjalne. Powinny być zmieniane co 30 dni (kategoria A – systemy i serwery o znaczeniu strategicznym);
2) hasła nie mogą zawierać imion, nazwisk, nazw własnych ani żadnych innych popularnych lub możliwych do odgadnięcia słów;
3) nie wolno udostępniać ani dopuścić do ujawnienia hasła;
4) zarówno obecne, jak i wszystkie nieaktualne hasła objęte są ścisłą tajemnicą;
5) hasła dostępu do baz danych oraz hasła administracyjne do serwerów i aplikacji wewnętrznych systemów informatycznych przetwarzających dane osobowe należy zmieniać co 30 dni, o ile nie ma ważnych przeciwskazań natury technologicznej. Hasła do pozostałych systemów powinny być zmieniane nie rzadziej niż co 3 miesiące. Dodatkowo obowiązuje zmiana wszystkich haseł administracyjnych każdorazowo w sytuacji stwierdzenia możliwego naruszenia bezpieczeństwa systemów informatycznych lub danych osobowych, podejrzenia ujawnienia któregoś z haseł lub odejścia z zespołu Administratora;
6) kopie aktualnych haseł administracyjnych (do kont, serwerów, systemów, aplikacji oraz baz danych) powinny być deponowane w zaklejonej kopercie/kopertach w bezpiecznym, niedostępnym dla osób nieuprawnionym miejscu.

§ 19. W przypadku cofnięcia operatorowi danych prawa do przetwarzania danych osobowych (np. w związku ze zmianą zakresu obowiązków lub stanowiska, rozwiązaniem umowy o pracę lub zakończeniem współpracy) obowiązują następujące zasady:

1) zobowiązania do nierozpowszechniania i niewykorzystywania poufnych informacji zdobytych w trakcie wykonywania powierzonych prac zachowują ważność także po cofnięciu uprawnień;
2) operator musi zwrócić wszelkie dokumenty i inne materiały dotyczące zbiorów i baz danych osobowych, przetwarzanych danych osobowych lub stosowanych zabezpieczeń;
3) z chwilą cofnięcia uprawnienia do przetwarzania danych osobowych wszystkie identyfikatory wykorzystywane przez operatora danych zostają, we współpracy z Administratorem Danych, zablokowane i wyrejestrowane z systemów, a wszystkie hasła z nimi powiązane tracą ważność;

4) identyfikatory są przechowywane i nie są przydzielane żadnemu innemu operatorowi danych.

Rozdział 4

Procedury rozpoczęcia, zakończenia pracy i obsługi komputera

§ 20. 1. Każdorazowo przy rozpoczęciu pracy operatorzy danych mają obowiązek podać hasło startowe komputera, a następnie zalogować się do systemu informatycznego (system operacyjny lub aplikacja) w którym przetwarzane są dane osobowe.

2. Operator danych rozpoczynając pracę zobowiązany jest dopilnować, czy zostało uruchomione oprogramowanie antywirusowe monitorujące komputer, jeśli takowe jest dostępne.

3. Wszelkie zauważone okoliczności wskazujące na możliwość naruszenia bezpieczeństwa danych osobowych muszą zostać bezzwłocznie zgłoszone do Administratora Danych.

§ 21. 1. Jeśli istnieje taka możliwość, to muszą być stosowane wygaszacze ekranu zabezpieczone hasłem. Wygaszacz powinien się włączyć automatycznie po maks. 10 minutach bezczynności, dodatkowo operator danych powinien mieć możliwość ręcznego włączenia wygaszacza, do czego jest również zobowiązany przy opuszczaniu stanowiska pracy przy komputerze.

2. Wyłączenie wygaszacza ekranu wymaga podania hasła operatora danych lub administratora komputera na którym wygaszacz został uruchomiony.

§ 22. 1. Po zakończeniu pracy operator danych oraz administrator jest zobowiązany wylogować się z aplikacji/systemu oraz zabezpieczyć komputer przed dostępem do danych przez osoby nieuprawnione.

2. W uzasadnionych przypadkach administratorzy mogą uzyskać od Administratora Danych lub Administratora Systemu Informatycznego zgodę na odstępstwa od zasad opisanych w punkcie poprzedzającym, w zakresie konieczności wylogowywania się z aplikacji lub systemów.

Rozdział 5

Komputery przenośne wykorzystywane do przetwarzania danych osobowych

§ 23. 1. Osoba użytkująca komputer przenośny, służący do przetwarzania danych osobowych, zobowiązana jest zachować szczególną ostrożność podczas transportu oraz używania komputera poza siedzibą Administratora Danych, w celu uniemożliwienia dostępu do zgromadzonych i przetwarzanych na nim danych przez osoby nieupoważnione, a w szczególności:

1) nie zezwalać na korzystanie z komputera osobom, które nie posiadają upoważnienia do przetwarzania danych osobowych wydanego przez Administratora Danych;
2) przewozić lub przenosić komputer z zachowaniem koniecznych wymogów bezpieczeństwa, w szczególny sposób chroniąc go przed utratą;
3) w przypadku zgubienia lub kradzieży komputera użytkownik zobowiązany jest niezwłocznie powiadomić o tym fakcie Administratora Danych.

2. Komputer musi zostać skonfigurowany tak, aby do jego uruchomienia wymagane było podanie hasła startowego BIOS, a start systemu operacyjnego możliwy był jedynie z wewnętrznego dysku.

3. O ile to możliwe należy uruchomić mechanizmy kryptograficzne (sprzętowe lub programowe) pozwalające na szyfrowanie danych znajdujących się na wewnętrznym dysku.

4. Na wszystkich kartach sieciowych (Ethernet, WiFi, IR, Bluetooth, FireWire, modem, itp) należy skonfigurować i uruchomić oprogramowanie firewall, ograniczając do niezbędnego minimum możliwość inicjowania połączeń sieciowych z zewnątrz do komputera.

Rozdział 6

Metody i częstotliwość sprawdzania obecności niebezpiecznego oprogramowania na stanowiskach operatorów danych oraz sposoby ich usuwania

§ 24. 1. Wszystkie komputery i stacje robocze, na których operatorzy danych przetwarzają dane osobowe, należy wyposażyć w aktualizowane automatycznie oprogramowanie antywirusowe sprawdzające aktywnie funkcjonowanie systemów operacyjnych, przetwarzanych plików danych oraz podłączanych nośników danych, w celu wykrycia obecności lub identyfikacji podatności na działanie złośliwego oprogramowania.

2. W przypadku wykrycia nieprawidłowości w zakresie opisanym w punkcie 1, należy niezwłocznie powiadomić Administratora Danych.

Rozdział 7

Metody i częstotliwość aktualizacji i instalacji oprogramowania systemowego oraz aplikacji na stanowiskach operatorów danych

§ 25. Na wszystkich komputerach i stacjach roboczych, na których operatorzy danych przetwarzają dane osobowe, obowiązują następujące zasady:

1) system operacyjny instaluje i konfiguruje osoba upoważniona przez Administratora Danych;
2) urządzenia, które w trakcie udostepnienia i aplikowania poprawek nie były włączone powinny zostać zaktualizowane po uruchomieniu i restartowane po zakończeniu procesu;
3) operatorzy danych nie są upoważnieni do samodzielnego instalowania na swoich stanowiskach aplikacji i oprogramowania użytkowego;
4) aktualizacja aplikacji i oprogramowania użytkowego odbywa się w trybie automatycznym lub manualnym, pod nadzorem osoby upoważnionej przez Administratora Danych.

§ 26. Z wyjątkiem uzasadnionym przypadków, potwierdzonych decyzją Administratora Danych, operatorzy danych nie posiadają uprawnień administracyjnych do swoich komputerów.

§ 27. W przypadku wykrycia nieprawidłowości w zakresie opisanym w niniejszym rozdziale, należy niezwłocznie powiadomić Administratora Danych.

Rozdział 8

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

§ 28. 1. Kopie awaryjne powinny być wykonywane regularnie i zgodnie z przyjętym harmonogramem przez upoważnionego administratora systemu lub inną upoważnioną osobę. Po sporządzeniu powinno się sprawdzić wykonaną kopię pod kątem jej prawidłowości i możliwości odtworzenia danych.

2. Kopie awaryjne powinny być okresowo sprawdzane pod kątem przydatności do odtworzenia danych w przypadku awarii systemu.

3. Kopie zapasowe baz danych osobowych powinny być przechowywane według poniższej specyfikacji:

1) backup online baz danych - synchronizacja baz danych w trybie master-slave;
2) backup dzienny baz danych - przechowywany w oddzielnych lokalizacjach;
3) backup miesięczny baz danych - pełny, według stanu bieżącego, kasowany po ustalonym okresie od daty wykonania.

4. Kopie danych opisane w ust. 3 powinny być przechowywane na dyskach lokalnych lub macierzach serwerów wykonujących backup lub magazynujących dane.

5. Serwery i repozytoria danych powinny się znajdować w strefach przetwarzania danych osobowych.

§ 29. Dla systemów finansowo-kadrowych kopie bezpieczeństwa wykonuje się nie rzadziej, niż raz na miesiąc. Dla pozostałych danych o częstotliwości decydują administratorzy systemów, w których te dane są przechowywane, w zależności od liczby wprowadzanych zmian, nie rzadziej jednak niż raz na dwa miesiące. Kopie zapasowe przechowuje się w zamkniętej szafie.

§ 30. 1. W przypadku konieczności oddania dysku lub innego nośnika danych osobowych do serwisu, Administrator Danych lub inna upoważniona osoba pod jego nadzorem, powinna wymazać zawartość nośnika tak, by nie dało się jej odzyskać. Jeśli skasowanie danych jest niemożliwe lub nie daje pewności usunięcia, nośnik taki powinien być zniszczony, a nie serwisowany.

2. W uzasadnionych przypadkach (np. wysoka cena nośnika, który powinien być, zgodnie z ust. 7, zniszczony) istnieje możliwość wykonania naprawy nośnika danych, na którym znajdują się nieusunięte dane osobowe, ale czynność taka musi odbywać pod nadzorem Administratora Danych, Procesora lub na mocy osobnego porozumienia z wykonującym serwis. Porozumienie takie musi zawierać zapisy związane z ochroną danych osobowych przetwarzanych przez Administratora Danych. Jeśli to możliwe powinno być sporządzone zgodnie ze wzorem określonym w załączniku na 14 do Polityki.

§ 31. Wszelkie nośniki, które podlegają niszczeniu, w tym uszkodzone dyski twarde, muszą zostać zniszczone komisyjnie przy udziale Administratora Danych lub jego przedstawiciela tak, by nie dało się w żaden sposób odzyskać tych danych.

§ 32. Kopie danych osobowych na papierze i na innych nośnikach danych mogą być wykonywane tylko w sytuacji wynikających z przepisów i procedur wewnętrznych (np. na

życzenie użytkownika którego dane dotyczą lub na wniosek osób i instytucji uprawnionych). Wydruki należy przechowywać z zachowaniem wszelkich środków ostrożności i muszą zostać one skutecznie zniszczone zaraz po ich wykorzystaniu oraz ustaniu powodu przetwarzania na nich danych osobowych.

Rozdział 9

Sposób dokonywania przeglądów i konserwacji systemów przetwarzania danych osobowych

§ 33. 1. Operacje związane z dokonywaniem przeglądów i konserwacji systemów przetwarzających dane osobowe wykonywane są pod nadzorem Administratora Danych.

2. Administrator Danych zobowiązany jest do wyznaczenia osób upoważnionych do dokonywania przynajmniej raz w miesiącu pod nadzorem, całościowego przeglądu i konserwacji wykorzystywanych systemów.

§ 34. W przypadku wykrycia nieprawidłowości w działaniu systemów, związanych z naruszeniem mechanizmów ochrony, niezwłocznie podejmowane są działania określone w Instrukcji postepowania w przypadku naruszenia ochrony danych osobowych – zał. Nr 21 do Polityki Bezpieczeństwa.

Rozdział 10

Sposoby postępowania w zakresie komunikacji w sieci komputerowej

§ 35. Dane osobowe przetwarzane przez serwery powinny być przesyłane za pośrednictwem sieci komputerowych w postaci zaszyfrowanej lub przy użyciu transmisji kodowanej.

§ 36. Dostęp do sieci wewnętrznych (biurowej) i wszystkich urządzeń je obsługujących powinny mieć jedynie uprawnione osoby posiadające upoważnienie nadane przez Administratora Danych.

§ 37. Bazy danych w których przetwarzane są dane osobowe powinny być skonfigurowane tak, aby pozwalały na połączenia tylko z wcześniej określonych komputerów. Wszelkie inne próby dostępu muszą zostać zalogowane i sprawdzone przez Administratora Systemu Informatycznego. W przypadku stwierdzenia prób połączenia z nieuprawnionego komputera należy niezwłocznie podjąć czynności wyjaśniające oraz powiadomić Administratora Danych.

Rozdział 11

Zabezpieczenie zasilania systemów przetwarzających dane osobowe

§ 38. 1. Serwery i urządzenia uczestniczące w przetwarzaniu danych osobowych, w szczególności te na których zainstalowane są bazy danych osobowych lub funkcjonują repozytoria danych, powinny być podłączone do awaryjnych źródeł zasilania (UPS) lub posiadać własne, niezależne źródła zasilania, pozwalających na ich awaryjną pracę przez okres czasu wystarczający do pełnego, automatycznego zamknięcia systemu, gwarantującego zachowanie integralności danych osobowych.

2. O ile to możliwe urządzenia opisane w punkcie poprzedzającym powinny być podłączone do dwóch niezależnych, gwarantowanych źródeł zasilania.

3. Nadzór nad funkcjonowaniem systemu zasilania urządzeń sprawuje Administrator Danych w zakresie sprzętu biurowego, serwerów oraz Procesor w stosunku do platformy hostingowej.

Rozdział 12

Rejestracja i monitoring dostępu do systemów przetwarzania danych osobowych

§ 39. 1. Każdorazowy dostęp do baz danych osobowych oraz serwerów, na których przetwarzane są dane osobowe powinien być odnotowywany w logach/rejestrach. System rejestracji powinien w pełni pozwalać na identyfikację tożsamości operatora danych, aplikacji lub administratora, który w danym czasie uzyskał dostęp do systemów przetwarzających dane osobowe i/lub dokonał operacji na danych.

2. Administrator Danych, a na jego zlecenie Administrator Systemu Informatycznego, lub osoba przez nich wyznaczona, zobowiązani są do bieżącego monitorowania logów. Wszelkie próby nieuprawnionego dostępu muszą być zgłaszane Administratorowi Danych zgodnie z Instrukcją postępowania w przypadku naruszenia ochrony danych osobowych.

3. Kopie zapasowe logów/rejestrów powinny być tworzone automatycznie i powinny być przechowywane.

Rozdział 13

Zasady ogólne

§ 40. Wszystkie czynności związane z przetwarzaniem danych osobowych w Centrum Integracji Społecznej w Świętochłowicach, które nie zostały opisane w niniejszej Instrukcji, są nadzorowane przez Administratora Danych.

§ 41. Administrator Danych posiada uprawnienia do zmian regulacji wynikających z niniejszego dokumentu.

§ 42. Administrator Danych może powierzyć (osobie trzeciej, w tym Procesorowi lub innej osobie lub podmiotowi) całość lub część czynności związanych z nadzorem nad funkcjonowaniem części lub całości systemów i procesów związanych z przetwarzaniem danych osobowych w ramach prowadzonej działalności. W każdym przypadku na Administratorze Danych lub osobie przez nią upoważnionej ciąży obowiązek kontrolowania właściwego wykonywania czynności związanych z przetwarzaniem danych osobowych.

Załącznik nr 2

WZÓR

ELEKTRONICZNY REJESTR CZYNNOŚCI PRZETWARZANIA

Lp.	Dział, zespół, stano-wisko	Stosowane oprogramo-wanie	Czynność przetwa-rzania	Właściciel procesu (danych)	Cel przetwa-rzania	Kategorie osób, których dane dotyczą	Kategorie danych osobowych	Kategorie odbiorców - innych niż podmiot przetwarzający (w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych)	Lokali-zacja danych	Podstawa przetw-arzania	Przekazywa-nie danych do państwa trzeciego lub organizacji międzynaro-dowych	Adekwatne zabezpie-czenia wymagane od państw trzecich	Okres przechowywania danych - planowane terminy usunięcia danych, jeżeli są możliwe do podania	Opis technicznych i organizacyj-nych środków bezpieczeń-stwa (art. 30 ust. 1 pkt g)

Załącznik nr 3

WYTYCZNE W ZAKRESIE OCENY RYZYKA

1. Szacowanie ryzyka w zakresie prawdopodobieństwa wystąpienia zdarzenia powodującego naruszenie bezpieczeństwa danych osobowych jest dokonywane przez wyrażenie poziomu ryzyka jako iloczynu prawdopodobieństwa wystąpienia zdarzenia oraz jego skutku korzystając z metody zarządzania ryzykiem w systemach zarządzania bezpieczeństwem informacji w urzędach administracji rządowej rekomendowanej przez Komitet Rady Ministrów ds. Cyfryzacji:

$$Rp = P \times (Sd + Si + Sp)$$

gdzie:

Rp – poziom wyliczanego ryzyka,

P – wartość przypisana prawdopodobieństwu materializacji zagrożenia z zakresu {0, 1, 2, 3,4}, gdzie:

0 – zdarzenie nieprawdopodobne,

1 – zdarzenie prawie nieprawdopodobne,

2 – zdarzenie mało prawdopodobne,

3 – zdarzenie wysoce prawdopodobne,

4 – zdarzenie niemal pewne.

Sd, Si, Sp – skutki zdarzenia odpowiednio w zakresie dostępności informacji, integralności oraz poufności z zakresu {0, 1, 2, 3, 4}, gdzie:

0 – zdarzenie nie powoduje skutku (nie występuje),

1 – zdarzenie wywołuje niewielki skutek,

2 – zdarzenie wywołuje znaczący skutek,

3 – zdarzenie wywołuje bardzo znaczący skutek,

4 – zdarzenie wywołuje skutek katastrofalny.

Wartość	Poziom ryzyka
1-12	NISKI poziom ryzyka utraty bezpieczeństwa danych osobowych
13-23	ŚREDNI poziom ryzyka utraty bezpieczeństwa danych osobowych
24-36	WYSOKI poziom ryzyka utraty bezpieczeństwa danych osobowych
36-48	MAKSYMALNY poziom ryzyka utraty bezpieczeństwa danych osobowych

2. Poziomy ryzyka utraty bezpieczeństwa danych osobowych:

a) NISKI – niskie szkody w przypadku realizacji zagrożenia i niska możliwość jego wystąpienia;

b) ŚREDNI – wysokie szkody w przypadku realizacji zagrożenia i niska możliwość jego realizacji bądź niskie szkody w przypadku realizacji zagrożenia i wysoka możliwość jego realizacji;

c) WYSOKI – wysokie szkody w przypadku realizacji zagrożenia i wysoka możliwość jego wystąpienia;

d) MAKSYMALNY – wysokie szkody w przypadku realizacji zagrożenia oraz wysoka możliwość jego wystąpienia, skutkująca nie tylko na organizację, ale na podmioty trzecie.

Załącznik nr 4

WZÓR

WYKAZ KONT OSÓB I SYSTEMÓW PRZETWARZAJĄCYCH DANE OSOBOWE

Lp.	Imię i nazwisko/nazwa systemu lub aplikacji	Zbiór danych którego uprawnienia dotyczą	Identyfikator użytkownika/konta w systemie informatycznym	Data przyznania uprawnień	Data cofnięcia uprawnień	UWAGI

Załącznik nr 5

WZÓR

ZGŁOSZENIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH DO ORGANU NADZORCZEGO

Dane Administratora Danych Osobowych		Nazwa organu nadzorczego	Data naruszenia	Godzina naruszenia
1	Imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych Osobowych			
2	Kategorie i przybliżona ilość osób, których dane dotyczą			
3	Kategorie i przybliżona ilość wpisów danych osobowych, których dotyczy naruszenie			
4	Środki zastosowane przez Administratora Danych Osobowych w celu zaradzenia naruszeniu (w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków)			
5	Okoliczności naruszenia			
6	Charakter naruszenia			
7	Możliwe konsekwencje naruszenia			

Data i podpis Inspektora Ochrony Danych Osobowych: .....

Załącznik nr 6

WZÓR

SPRAWOZDANIE ZE SPRAWDZENIA ZGODNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH Z PRZEPISAMI ODO

1	Oznaczenie Administratora Danych Osobowych i adres jego siedziby (pełna nazwa i adres)	
2	Imię i nazwisko Inspektora Ochrony Danych Osobowych	
3	Data rozpoczęcia i zakończenia sprawdzenia	
4	Określenie przedmiotu i zakresu sprawdzenia	
5	Wykaz czynności podjętych przez Inspektora Ochrony Danych Osobowych w toku sprawdzenia oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach	
6	Opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych	
7	Stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych	

	w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem	
8	Wyszczególnienie załączników stanowiących składową część sprawozdania	

.....

data i podpis Inspektora Ochrony Danych Osobowych

.....

data i podpis Administratora Danych Osobowych

Załącznik nr 7

KLAUZULA ZGODY NA PRZETWARZANIE DANYCH OSOBOWYCH

1. Administratorem Pani/Pana danych osobowych jest:

Centrum Integracji Społecznej w Świętochłowicach

2. Inspektorem Ochrony Danych Osobowych w Centrum Integracji Społecznej w Świętochłowicach jest:

Mirosław Karwot; email: iod.inspect@gmail.com

3. Pani/Pana dane osobowe przetwarzane będą w celu oraz zakresie niezbędnym do jego realizacji. Cel i podstawa prawna przetwarzania danych osobowych:

Dane osobowe będą przetwarzanie w celu .....
Podstawa prawna przetwarzania danych osobowych:
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE
- Kodeks cywilny (art. 23 i 24)

4. Odbiorcą Pani/Pana danych osobowych będą:

Centrum Integracji Społecznej w Świętochłowicach.
Organy władzy publicznej oraz podmioty wykonujące zadania publiczne lub działające na zlecenie organów władzy publicznej, w zakresie i w celach, które wynikają z przepisów powszechnie obowiązującego prawa.
Inne podmioty, które na podstawie umów podpisanych z Centrum Integracji Społecznej w Świętochłowicach przetwarzają dane osobowe dla których Administratorem jest Centrum Integracji Społecznej w Świętochłowicach.

5. Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego/organizacji międzynarodowej.

6. Pani/Pana dane osobowe będą przechowywane przez okres:

Trwania umowy. Po rozwiązaniu umowy dane będą przechowywane ze względu na obowiązki wynikające z regulacji księgowych i podatkowych przez czas ich trwania oraz ze względów bezpieczeństwa prawnego, do czasu przedawnienia ewentualnych roszczeń przez okres wymagany przez przepisy powszechnie obowiązującego prawa.

7. Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania (jeżeli przetwarzanie odbywa się na podstawie zgody), którego dokonano na podstawie zgody przed jej cofnięciem.

8. Ma Pan/Pani prawo wniesienia skargi do organu nadzorczego, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.

9. Podanie przez Pana/Panią danych osobowych jest (wybrać odpowiednio):

	wymogiem ustawowym
	warunkiem umownym
v	warunkiem zawarcia umowy

10. Jest Pan/Pani zobowiązana do ich podania, a konsekwencją niepodania danych będzie:

Brak możliwości zawarcia umowy.

11. Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany i nie będzie przeprowadzany proces profilowania.

Wyrażenie zgody	
Imię i nazwisko osoby wyrażającej zgodę:	
Data:	
Zapoznałam/zapoznałem się z Klauzulą Informacyjną Administratora danych i wyrażam zgodę na przetwarzanie moich danych osobowych w wyżej wymienionym celu i zakresie.	
Podpis osoby wyrażającej zgodę:	

Załącznik nr 8

WZÓR

REJESTR INCYDENTÓW NARUSZENIA OCHRONY DANYCH

Lp.	Data wystąpienia incydentu	Krótki opis incydentu	Osoba zgłaszająca incydent	Miejsce wystąpienia incydentu	Zbiór danych, którego dotyczy incydent	Status sprawy

Załącznik nr 9

WZÓR

WYKAZ POMIESZCZEŃ, W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE

Lp.	Lokalizacja (adres i określenie pomieszczenia)	Dział/osoba użytkująca pomieszczenie	Zabezpieczenie pomieszczenia

Załącznik nr 10

ZGODA NA UPUBLICZNIENIE WIZERUNKU

1. Administratorem Pani/Pana danych osobowych jest:

Centrum Integracji Społecznej w Świętochłowicach

2. Inspektorem Ochrony Danych Osobowych w Centrum Integracji Społecznej w Świętochłowicach jest:

Mirosław Karwot; email: iod.inspect@gmail.com

3. Zakres przetwarzanych danych:

Zdjęcia i materiały filmowe zawierające wizerunek, zarejestrowane podczas wydarzeń związanych z uczestnictwem w programach, projektach i innych uroczystościach zorganizowanych przez Centrum Integracji Społecznej w Świętochłowicach, udostępnione na stronie internetowej Centrum Integracji Społecznej w Świętochłowicach, profilach internetowych, w mediach społecznościowych zarządzanych przez Centrum Integracji Społecznej w Świętochłowicach oraz w innych mediach, a także w gazetkach i na tablicach informacyjnych.

4. Pani/Pana dane osobowe przetwarzane będą w celu oraz zakresie niezbędnym do jego realizacji. Cel i podstawa prawna przetwarzania danych:

Informacja oraz promocja Centrum Integracji Społecznej w Świętochłowicach.
Podstawa prawna przetwarzania danych osobowych:
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.
Ustawa o prawach autorskich i prawach pokrewnych (art. 81 i 83).
Kodeks Cywilny (art. 23 i 24).

5. Odbiorcą Pani/Pana danych osobowych będą (kategorie odbiorców):

Osoby korzystające z strony internetowej Centrum Integracji Społecznej w Świętochłowicach, profili internetowych, mediów społecznościowych zarządzanych przez Centrum Integracji Społecznej w Świętochłowicach oraz innych mediów, a także z gazetek i tablic informacyjnych.

6. Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego/organizacji międzynarodowej.

7. Pani/Pana dane osobowe będą przechowywane przez okres:

Do wycofania zgody.

8. Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na

Załącznik nr 11

WZÓR

WYKAZ UDOSTĘPNIEŃ DANYCH OSOBOWYCH INNYM PODMIOTOM

Lp.	Imię i nazwisko/nazwa zbioru (możliwie najpełniejszy opis osoby, której dane zostały udostępnione lub całego zbioru)	Data udostępnienia	Nazwa podmiotu, któremu udostępniono dane (np. upoważniony organ, instytucja lub inny podmiot, który wykazał uprawnienie do udostępnienia mu danych)	Cel udostępnienia (podstawa prawna/nr umowy)	Zakres udostępnionych danych (jakie dane zostały udostępnione)	Rodzaj zbioru/zasobu i jego lokalizacja (np. papierowy wydruk, dane w formie elektronicznej)

zgodność z prawem przetwarzania (jeżeli przetwarzanie odbywa się na podstawie zgody), którego dokonano na podstawie zgody przed jej cofnięciem.

9. Ma Pan/Pani prawo wniesienia skargi do organu nadzorczego, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych dotyczących Pani/Pana narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.

10. Podanie przez Pana/Panią danych swoich osobowych jest (wybrać odpowiednio):

	wymogiem ustawowym
v	warunkiem umownym
	warunkiem zawarcia umowy

11. Jest Pan/Pani zobowiązana do ich podania, a konsekwencją niepodania danych osobowych będzie:

Brak obowiązku.

12. Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany i nie będzie przeprowadzany proces profilowania.

Wyrażenie zgody	
Imię i nazwisko osoby wyrażającej zgodę:	
Data:	
Zapoznałam/zapoznałem się z Klauzulą Informacyjną Administratora danych i wyrażam zgodę na przetwarzanie moich danych osobowych w wyżej wymienionym celu i zakresie.	
Podpis osoby wyrażającej zgodę:	

Załącznik nr 12

WZÓR

WYKAZ UDOSTĘPNIEŃ DANYCH OSOBOM, KTÓRYCH DOTYCZĄ

Lp.	Imię i nazwisko osoby, której dane są udostępniane	Data udostępnienia	Rodzaj zbioru / zasobu i jego lokalizacja (np. papierowy wydruk danych zawartych w określonym zbiorze)

Załącznik nr 13

WZÓR

WNIOSEK O UDOSTĘPNIENIE DANYCH OSOBOWYCH

1	Wnioskodawca (nazwa firmy lub jednostki, osoby fizycznej, adres siedziby lub zamieszkania, NIP, KRS)	
2	Podstawa prawna upoważniająca do pozyskania danych albo wskazanie wiarygodnie uzasadnionej potrzeby posiadania danych	
3	Opis lub nazwa zbioru, z którego dane mają być udostępnione	
4	Zakres żądanych danych	
5	Informacje umożliwiające wyszukanie w zbiorze danych	

Załącznik nr 14

WZÓR

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w Świętochłowicach w dniu ..... pomiędzy

Gminą Świętochłowice, 41-600 Świętochłowice, ul. Katowicka 54, NIP: 6272748728 reprezentowaną przez ....., Dyrektora Centrum Integracji Społecznej w Świętochłowicach, zwanym dalej Powierzającym,

a

....., NIP ....., zwanym dalej Przetwarzającym.

Strony niniejszym zawierają Umowę powierzenia przetwarzania danych osobowych o następującej treści:

§ 1

Oświadczenia Stron

1. Administrator Danych Osobowych powierza Przetwarzającemu do przetwarzania dane osobowe, które zgromadził zgodnie z obowiązującymi przepisami prawa i przetwarza w następujących zbiorach danych: pełny zakres zbiorów wynikający z działań prowadzonych w zakresie pełnienia funkcji Administratora Systemu Informatycznego.

2. Przetwarzający oświadcza, że dysponuje środkami umożliwiającymi prawidłowe przetwarzanie danych osobowych powierzonych przez Administratora Danych, w zakresie i celu określonym Umową.

3. Przetwarzający oświadcza również, że osobom zatrudnionym przy przetwarzaniu powierzonych danych osobowych nadane zostały upoważnienia do przetwarzania danych osobowych oraz że osoby te zostały zapoznane z przepisami o ochronie danych osobowych, oraz z odpowiedzialnością za ich nieprzestrzeganie, zobowiązały się do ich przestrzegania oraz do bezterminowego zachowania w tajemnicy przetwarzanych danych osobowych i sposobów ich zabezpieczenia.

§ 2

Cel, zakres, miejsce przetwarzania powierzonych danych osobowych

1. Administrator Danych powierza Przetwarzającemu przetwarzanie danych osobowych zawartych w zbiorach: pełny zakres zbiorów wynikający z działań prowadzonych w zakresie pełnienia funkcji Administratora Systemu Informatycznego

2. Przetwarzający będzie przetwarzał powierzone na podstawie umowy dane, jedynie w celu prawidłowego wykonywania umowy nr 2/CIS/2019.

3. Przetwarzający zobowiązuje się do przetwarzania powierzonych danych osobowych wyłącznie w celach związanych z realizacją Umowy i wyłącznie w zakresie, jaki jest niezbędny do realizacji tych celów.

4. Na wniosek Administratora Danych lub osoby, której dane dotyczą Przetwarzający wskaże miejsca, w których przetwarza powierzone dane.

§ 3

Zasady przetwarzania danych osobowych

1. Strony zobowiązują się wykonywać zobowiązania wynikające z niniejszej Umowy z najwyższą starannością zawodową w celu zabezpieczenia prawnego, organizacyjnego i technicznego interesów Stron w zakresie przetwarzania powierzonych danych osobowych.

2. Przetwarzający zobowiązuje się zastosować środki techniczne i organizacyjne mające na celu należyte, odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, zabezpieczenie powierzonych do przetwarzania danych osobowych, w szczególności zabezpieczyć je przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa, oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

3. Przetwarzający oświadcza, że zastosowane do przetwarzania powierzonych danych systemy informatyczne spełniają wymogi aktualnie obowiązujących przepisów prawa.

4. Przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora Danych.

5. Przetwarzający, biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga Administratorowi Danych poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw.

6. Przetwarzający, uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga Administratorowi Danych wywiązać się z obowiązków określonych w art. 32–

36 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych).

7. Przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji Administratora Danych usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że szczególne przepisy prawa nakazują przechowywanie danych osobowych.

8. Przetwarzający udostępnia Administratorowi Danych wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszej umowie oraz umożliwia Administratorowi Danych lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

9. Przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody Administratora Danych.

§ 4

Odpowiedzialność Stron

1. Administrator Danych ponosi odpowiedzialność za przestrzeganie przepisów prawa w zakresie przetwarzania i ochrony danych osobowych według rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

2. Powyższe nie wyłącza odpowiedzialności Przetwarzającego za przetwarzanie powierzonych danych niezgodnie z umową.

3. Przetwarzający odpowiada za szkody spowodowane przetwarzaniem, jeśli nie dopełnił obowiązków, które nakłada niniejsza umowa, lub gdy działał poza zgodnymi z prawem instrukcjami Administratora Danych lub wbrew tym instrukcjom.

§ 5

Postanowienia końcowe

1. Wszelkie zmiany niniejszej Umowy powinny być dokonane w formie pisemnej pod rygorem nieważności.

2. W zakresie nieuregulowanym niniejszą Umową zastosowanie mają przepisy Kodeksu Cywilnego.

3. W przypadku, gdy niniejsza Umowa odwołuje się do przepisów prawa, oznacza to również inne przepisy dotyczące ochrony danych osobowych, a także wszelkie nowelizacje, jakie wejdą w życie po dniu zawarcia Umowy, jak również akty prawne, które zastąpią wskazane ustawy i rozporządzenia.

4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

5. Niniejsza Umowa powierzenia przetwarzania danych obowiązuje na czas wykonywania przez Przetwarzającego czynności ujętych w Umowie.

.....	.....
data i podpis Powierzającego	data i podpis Przetwarzającego

Załącznik nr 15

WZÓR

WYKAZ PODMIOTÓW, Z KTÓRYMI ZAWARTO UMOWY POWIERZENIA PRZETWARZANIA DANYCH

Lp.	Nazwa podmiotu, któremu powierzono dane	Nr umowy powierzenia	Czas trwania powierzenia	Cel i charakter powierzenia	Rodzaj danych osobowych (zwykłe/wrażliwe)	Kategorie osób, których dane dotyczą

Załącznik nr 16

WZÓR

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH NR...

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1), niniejszym upoważniam do przetwarzania danych osobowych:

Imię i nazwisko:	
Stanowisko:	
W zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku	
Upoważnienie do przetwarzania danych osobowych zawartych w następujących zbiorach:	
Upoważnienie obejmuje uprawnienie do przetwarzania danych w zakresie (w tym miejscu należy wskazać kategorie danych oraz operacje na danych osobowych, jakich może dokonywać upoważniony do przetwarzania danych osobowych):	
Okres ważności upoważnienia:	
Podpis osoby nadającej upoważnienie:	

Załącznik nr 17

WZÓR

ZBIORY DANYCH OSOBOWYCH I ICH CHARAKTERYSTYKA

Zbiór	Opis	Pola informacyjne	Powiązania z innymi zbiorami	Narzędzia przetwarzania	Miejsce przetwarzania	Osoby przetwarzające	Podstawy prawne przetwarzania

Załącznik nr 18

WZÓR

WYKAZ PRZEPROWADZONYCH KONTROLI

Lp.	Imię i nazwisko przeprowadzającego kontrolę	Data kontroli	Zakres kontroli	UWAGI

Załącznik nr 19

WZÓR

OŚWIADCZENIE PRACOWNIKA PRZETWARZAJĄCEGO DANE OSOBOWE

W związku z nadanym mi upoważnieniami:

1) do przetwarzania danych osobowych,
2) obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych,

oświadczam, że znane mi są przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), zwanego dalej „rozporządzeniem 2016/679".

Oświadczam, że zapoznałam/-łem się z:

1) Polityką Bezpieczeństwa Danych Osobowych.
2) Instrukcją Zarządzania Systemami Informatycznym Służącym Do Przetwarzania Danych.

Oświadczam, że zobowiązuję się przestrzegać zasad ochrony danych osobowych podczas wykonywania obowiązków służbowych, w tym do:

1) Dołożenia wszelkich starań, aby przy wykonywaniu powierzonych mi obowiązków przetwarzane dane osobowe były chronione.
2) Przetwarzania danych osobowych zgodnie z obowiązującymi przepisami prawa i regulacjami wewnętrznymi.
3) Do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, również po ustaniu zatrudnienia
4) Do zabezpieczania przetwarzanych danych osobowych przed ich:
   a) udostępnieniem osobom nieupoważnionym
   b) zabraniem przez osobę nieupoważnioną
   c) przetwarzaniem z naruszeniem przepisów prawa
   d) nieuprawnioną zmianą lub zniszczeniem
   e) utratą
   f) uszkodzeniem

Jednocześnie przyjmuję do wiadomości, że w przypadku naruszenia niniejszej tajemnicy podlegam sankcjom wynikającym z przepisów Kodeksu Pracy do zwolnienia dyscyplinarnego włącznie oraz sankcjom wynikającym z Ustawy o Ochronie Danych Osobowych.

Imię i nazwisko pracownika:	
Data:	
Podpis pracownika:	

Załącznik nr 20

OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

1. Administrator Danych Osobowych decyduje o zastosowaniu odpowiednich środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych.

2. Informatyk wraz z wyznaczonymi Użytkownikami powinni przeprowadzać okresową analizę ryzyka dla systemu informatycznego i na tej podstawie przedstawiać Administratorowi Danych Osobowych propozycje dotyczące zastosowania środków technicznych celem zapewnienia właściwej ochrony przetwarzanych danych.

3. Określenia poziomu bezpieczeństwa systemu informatycznego powinien dokonać Informatyk.

4. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych.

5. Środki ochrony, zastosowane dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych, obejmują:

1) środki ochrony fizycznej (np. drzwi ochronne, firma ochroniarska, monitoring);
2) środki techniczne (np. firewall, antywirus, podtrzymanie zasilania UPS);
3) środki organizacyjne (np. utworzenie Instrukcji zarządzania systemem informatycznym).

6. Zalecane środki do zastosowania:

1) środki ochrony fizycznej danych:
   a) zbiór danych osobowych powinien być przechowywany w pomieszczeniu zabezpieczonym drzwiami zwykłymi,
   b) zbiór danych osobowych powinien być przechowywany w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej,
   c) pomieszczenia, w których przetwarzany jest zbiór danych osobowych powinne być wyposażone w system alarmowy przeciwwłamaniowy,
   d) dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych, powinien być kontrolowany przez system monitoringu z zastosowaniem kamer,

e) dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych powienien być w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony,

f) zbiór danych osobowych w formie papierowej powinien być przechowywany w zamkniętej szafie niemetalowej lub metalowej,

g) kopie zapasowe/archiwalne zbioru danych osobowych powinny być przechowywane w zamkniętej szafie niemetalowej lub metalowej, sejfie, lub kasie pancernej,

h) pomieszczenie, w którym przetwarzane są zbiory danych osobowych, powinno być zabezpieczone przed skutkami pożaru za pomocą wolnostojącej gaśnicy,

i) dokumenty zawierające dane osobowe po ustaniu przydatności powinny być niszczone w sposób mechaniczny za pomocą niszczarek dokumentów;

2) środki ochrony technicznej danych:

a) powinny być zastosowane urządzenia typu UPS chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania,

b) dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe powinien być zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,

c) powinny zostać zastosowane środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych,

d) powinny zostać zastosowane systemowe mechanizmy wymuszające okresową zmianę haseł,

e) należy zastosować system rejestracji dostępu do systemu/zbioru danych osobowych,

f) powinny zostać zastosowane środki ochrony przed szkodliwym oprogramowaniem,

g) powinien zostać zastosowany Firewall do ochrony dostępu do sieci komputerowej,

h) dostęp do zbioru danych osobowych powinien wymagać uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,

i) powinny zostać zastosowane systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego,

j) powinny zostać zastosowane kryptograficzne środki ochrony danych osobowych na urządzeniach przenośnych,

Załącznik nr 20

OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

1. Administrator Danych Osobowych decyduje o zastosowaniu odpowiednich środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych.

2. Informatyk wraz z wyznaczonymi Użytkownikami powinni przeprowadzać okresową analizę ryzyka dla systemu informatycznego i na tej podstawie przedstawiać Administratorowi Danych Osobowych propozycje dotyczące zastosowania środków technicznych celem zapewnienia właściwej ochrony przetwarzanych danych.

3. Określenia poziomu bezpieczeństwa systemu informatycznego powinien dokonać Informatyk.

4. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych.

5. Środki ochrony, zastosowane dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych, obejmują:

1) środki ochrony fizycznej (np. drzwi ochronne, firma ochroniarska, monitoring);
2) środki techniczne (np. firewall, antywirus, podtrzymanie zasilania UPS);
3) środki organizacyjne (np. utworzenie Instrukcji zarządzania systemem informatycznym).

6. Zalecane środki do zastosowania:

1) środki ochrony fizycznej danych:
   a) zbiór danych osobowych powinien być przechowywany w pomieszczeniu zabezpieczonym drzwiami zwykłymi,
   b) zbiór danych osobowych powinien być przechowywany w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej,
   c) pomieszczenia, w których przetwarzany jest zbiór danych osobowych powinne być wyposażone w system alarmowy przeciwwłamaniowy,
   d) dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych, powinien być kontrolowany przez system monitoringu z zastosowaniem kamer,

e) dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych powienien być w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony,

f) zbiór danych osobowych w formie papierowej powinien być przechowywany w zamkniętej szafie niemetalowej lub metalowej,

g) kopie zapasowe/archiwalne zbioru danych osobowych powinny być przechowywane w zamkniętej szafie niemetalowej lub metalowej, sejfie, lub kasie pancernej,

h) pomieszczenie, w którym przetwarzane są zbiory danych osobowych, powinno być zabezpieczone przed skutkami pożaru za pomocą wolnostojącej gaśnicy,

i) dokumenty zawierające dane osobowe po ustaniu przydatności powinny być niszczone w sposób mechaniczny za pomocą niszczarek dokumentów;

2) środki ochrony technicznej danych:

a) powinny być zastosowane urządzenia typu UPS chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania,

b) dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe powinien być zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,

c) powinny zostać zastosowane środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych,

d) powinny zostać zastosowane systemowe mechanizmy wymuszające okresową zmianę haseł,

e) należy zastosować system rejestracji dostępu do systemu/zbioru danych osobowych,

f) powinny zostać zastosowane środki ochrony przed szkodliwym oprogramowaniem,

g) powinien zostać zastosowany Firewall do ochrony dostępu do sieci komputerowej,

h) dostęp do zbioru danych osobowych powinien wymagać uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,

i) powinny zostać zastosowane systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego,

j) powinny zostać zastosowane kryptograficzne środki ochrony danych osobowych na urządzeniach przenośnych,

k) powinny zostać zastosowane wygaszacze ekranów z hasłem na stanowiskach, na których przetwarzane są dane osobowe,

l) powinny zostać zastosowane mechanizmy automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika;

3) środki organizacyjne:

a) osoby zatrudnione przy przetwarzaniu danych powinny zostać zaznajomione z przepisami dotyczącymi ochrony danych osobowych,

b) osoby zatrudnione przy przetwarzaniu danych osobowych powinny zostać przeszkolone w zakresie zabezpieczeń systemu informatycznego,

c) osoby zatrudnione przy przetwarzaniu danych osobowych powinny zostać zobowiązane do zachowania ich w tajemnicy,

d) monitory komputerów, na których przetwarzane są dane osobowe powinny być ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane, w uzasadnionych przypadkach należy zastosować speclajne filtry prywatyzujące na monitory,

e) kopie zapasowe zbioru danych osobowych powinny być przechowywane w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.

7. Za niedopełnienie obowiązków wynikających z niniejszego dokumentu pracownik ponosi odpowiedzialność na podstawie Kodeksu Pracy oraz Ustawy o Ochronie Danych Osobowych.

8. Wszystkie osoby upoważnione do przetwarzania danych osobowych mogą ponieść odpowiedzialność karną w sytuacji naruszenia zasad określonych w niniejszym dokumencie.

Załącznik nr 21

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Rozdział 1

Istota naruszenia danych osobowych

§ 1. 1. Incydentem w zakresie danych osobowych jest sytuacja powodująca utratę poufności, integralności lub dostępności przetwarzanych danych.

2. Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

1) nieautoryzowany dostęp do danych;
2) nieautoryzowane modyfikacje lub zniszczenie danych;
3) udostępnienie danych nieautoryzowanym podmiotom;
4) nielegalne ujawnienie danych;
5) pozyskiwanie danych z nielegalnych źródeł.

Rozdział 2

Postępowanie w przypadku naruszenia danych osobowych

§ 2. 1. Każdy pracownik, który stwierdzi lub podejrzewa fakt naruszenia danych osobowych, jest zobowiązany niezwłocznie zgłosić to swojemu bezpośredniemu przełożonemu. Przełożony zgłasza fakt Inspektorowi Ochrony Danych lub Administratorowi Danych.

2. Typowe sytuacje, gdy użytkownik powinien powiadomić Inspektora Ochrony Danych lub Administratora Danych:

1) ślady na drzwiach, oknach i szafach wskazujące na próbę włamania;
2) niszczenie dokumentacji bez użycia niszczarki;
3) fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie;
4) otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe;

5) stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD (otwarte szafy, biurka, regały, urządzenia archiwalne);
6) nie zostało wykonane wylogowanie z systemu po zakończeniu pracy;
7) pozostawienie dokumentów w drukarce, kserokopiarce, skanerze;
8) nie wykonanie w określonym terminie kopii bezpieczeństwa;
9) wykonywanie operacji na danych służbowych w celach prywatnych;
10) ustawienie monitorów w sposób umożliwiający wgląd osób postronnych w dane osobowe;
11) wynoszenie danych osobowych w wersji papierowej lub elektronicznej na zewnątrz firmy bez upoważnienia Administratora;
12) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej;
13) stwierdzona próba lub modyfikacja danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia;
14) telefoniczne próby wyłudzenia danych osobowych;
15) kradzież komputerów lub twardych dysków z danymi osobowymi;
16) utrata kontroli nad kopią danych osobowych;
17) maile zachęcające do ujawnienia identyfikatora i/lub hasła;
18) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
19) istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki";
20) przechowywane haseł do systemów w pobliżu komputera.

§ 3. Każdy pracownik, który stwierdzi fakt naruszenia danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia.

§ 4. W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowania zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Inspektora Ochrony Danych, Administratora Danych lub innej osoby upoważnionej przez Administratora danych.

§ 5. Administrator Systemu Informatycznego jest zobowiązany do informowania Inspektora Ochrony Danych o wszelkich anomaliach w pracy administrowanych przez siebie urządzeń, mogących być przyczyną lub skutkiem incydentu w zakresie danych osobowych.

§ 6. W przypadku naruszenia danych osobowych Inspektor Ochrony Danych podejmuje następujące kroki:

1) zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości i ciągłości pracy;
2) odbiera dokładną relację z zaistniałego naruszenia bezpieczeństwa danych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem;
3) nawiązuje kontakt ze specjalistami zewnętrznymi (jeśli zachodzi taka potrzeba).

§ 7. Inspektor Ochrony Danych dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych wypełniając Załącznik nr 8.

§ 8. Inspektor Ochrony Danych zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych) sporządzając raport z przeprowadzonych działań.

Rozdział 3

Odpowiedzialność za naruszenie danych osobowych

§ 9. Wobec osoby, która w przypadku naruszenia danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne lub porządkowe. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z aktualnie obowiązującym przepisami oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

Rozdział 4

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

§ 10. 1. W przypadku naruszenia ochrony danych osobowych, Administrator lub Inspektor Ochrony Danych bez zbędnej zwłoki, w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia zgłasza je Urzędowi Ochrony Danych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Wzór zgłoszenia stanowi Załącznik nr 5.

2. Zgłoszenie, o którym mowa w ust. 1 powinno:

1) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
2) zawierać imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych lub oznaczenie innego punktu kontaktowego z którego można uzyskać więcej informacji;
3) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
4) opisywać środki zastosowane lub proponowane przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

3. Jeżeli i w zakresie, w jakim informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.

4. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu na zweryfikowanie przestrzegania niniejszego artykułu.

Rozdział 5

Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

§ 11. 1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą o takim naruszeniu.

2.Zawiadomienie o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w § 10 ust. 2 pkt 2-4.

3.Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane w następujących przypadkach:

1) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
2) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;
3) wymagałoby ono niewspółmiernie dużego wysiłku.

4. W przypadku, o którym mowa w ust. 3, wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Załącznik nr 22

WZÓR

ZGODA NA UPUBLICZNIENIE WIZERUNKU DZIECKA/PODOPIECZNEGO

1. Administratorem danych osobowych Pani/Pana dziecka/podopiecznego jest:

Centrum Integracji Społecznej w Świętochłowicach.

2. Inspektorem Ochrony Danych Osobowych w Centrum Integracji Społecznej w Świętochłowicach jest:

Mirosław Karwot; email: iod.inspect@gmail.com

3. Zakres przetwarzanych danych:

Zdjęcia i materiały filmowe zawierające wizerunek, zarejestrowane podczas wydarzeń związanych z uczestnictwem w programach, projektach i innych uroczystościach zorganizowanych przez Centrum Integracji Społecznej w Świętochłowicach, udostępnione na stronie internetowej Centrum Integracji Społecznej w Świętochłowicach, profilach internetowych, w mediach społecznościowych zarządzanych przez Centrum Integracji Społecznej w Świętochłowicach oraz w mediach, a także w gazetkach i na tablicach informacyjnych.

4. Dane osobowe Pani/Pana dziecka/podopiecznego przetwarzane będą w celu oraz zakresie niezbędnym do jego realizacji. Cel i podstawa prawna przetwarzania danych osobowych:

Informacja oraz promocja Centrum Integracji Społecznej w Świętochłowicach.
Podstawa prawna przetwarzania danych osobowych:
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.
Ustawa o prawach autorskich i prawach pokrewnych (art. 81 i 83). Kodeks Cywilny (art. 23 i 24).

5. Odbiorcą danych osobowych Pani/Pana dziecka/podopiecznego będą:

Osoby korzystające z strony internetowej Centrum Integracji Społecznej w Świętochłowicach, profili internetowych, mediów społecznościowych zarządzanych przez Centrum Integracji Społecznej w Świętochłowicach oraz innych mediów, a także z gazetek i tablic informacyjnych.

6. Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego/organizacji międzynarodowej.

7. Dane osobowe Pani/Pana dziecka/podopiecznego będą przechowywane przez okres:

Do wycofania zgody.

8. Posiada Pani/Pan prawo dostępu do treści danych osobowych Pani/Pana dziecka/podopiecznego oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania (jeżeli przetwarzanie odbywa się na podstawie zgody), którego dokonano na podstawie zgody przed jej cofnięciem.

9. Ma Pan/Pani prawo wniesienia skargi do organu nadzorczego, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dziecka/podopiecznego narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.

10. Podanie przez Pana/Panią danych osobowych Pani/Pana dziecka/podopiecznego jest:

	wymogiem ustawowym
v	warunkiem umownym
	warunkiem zawarcia umowy

11. Jest Pan/Pani zobowiązana do ich podania, a konsekwencją niepodania danych osobowych będzie:

Nie dotyczy.

12. Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany i nie będzie przeprowadzany proces profilowania.

Wyrażenie zgody	
Imię i nazwisko osoby wyrażającej zgodę:	
Data:	
Zapoznałam/zapoznałem się z Klauzulą Informacyjną Administratora danych i wyrażam zgodę na przetwarzanie danych osobowych mojego dziecka/podopiecznego zawierających wizerunek w wyżej wymienionym celu i zakresie.	
Podpis osoby wyrażającej zgodę:	

Załącznik nr 23

WZÓR

KLAUZULA ZGODY NA PRZETWARZANIE DANYCH OSOBOWYCH DZIECKA/PODOPIECZNEGO

1. Administratorem danych osobowych Pani/Pana dziecka/podopiecznego jest:

Centrum Integracji Społecznej w Świętochłowicach.

2. Inspektorem Ochrony Danych Osobowych w Centrum Integracji Społecznej w Świętochłowicach jest:

Mirosław Karwot; email: iod.inspect@gmail.com

3. Dane osobowe Pani/Pana dziecka/podopiecznego przetwarzane będą w celu oraz zakresie niezbędnym do jego realizacji. Cel i podstawa prawna przetwarzania danych osobowych:

Dane osobowe będą przetwarzanie w celu .....
Podstawa prawna przetwarzania danych osobowych:
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.
Kodeks Cywilny (art. 23 i 24).

4. Odbiorcą danych osobowych Pani/Pana dziecka/podopiecznego będą:

Centrum Integracji Społecznej w Świętochłowicach.
Organy władzy publicznej oraz podmioty wykonujące zadania publiczne lub działające na zlecenie organów władzy publicznej, w zakresie i w celach, które wynikają z przepisów powszechnie obowiązującego prawa.
Inne podmioty, które na podstawie umów podpisanych z Centrum Integracji Społecznej w Świętochłowicach przetwarzają dane osobowe dla których Administratorem jest Centrum Integracji Społecznej w Świętochłowicach.

5. Dane osobowe Pani/Pana dziecka/podopiecznego nie będą przekazywane do państwa trzeciego/organizacji międzynarodowej.

6. Dane osobowe Pani/Pana dziecka/podopiecznego będą przechowywane przez okres:

Trwania umowy. Po rozwiązaniu umowy dane będą przechowywane ze względu na obowiązki wynikające z regulacji księgowych i podatkowych przez czas ich trwania oraz ze względów bezpieczeństwa prawnego, do czasu przedawnienia ewentualnych roszczeń przez okres wymagany przez przepisy powszechnie obowiązującego prawa.

7. Posiada Pani/Pan prawo dostępu do treści danych osobowych Pani/Pana dziecka/podopiecznego oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania,

prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania (jeżeli przetwarzanie odbywa się na podstawie zgody), którego dokonano na podstawie zgody przed jej cofnięciem.

8. Ma Pan/Pani prawo wniesienia skargi do organu nadzorczego, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dziecka/podopiecznego narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.

9. Podanie przez Pana/Panią danych osobowych Pani/Pana dziecka/podopiecznego jest:

	wymogiem ustawowym
	warunkiem umownym
v	warunkiem zawarcia umowy

10. Jest Pan/Pani zobowiązana do ich podania, a konsekwencją niepodania danych osobowych będzie:

Brak możliwości zawarcia umowy.

11. Dane osobowe Pani/Pana dziecka/podopiecznego nie będą przetwarzane w sposób zautomatyzowany i nie będzie przeprowadzany proces profilowania.

Wyrażenie zgody	
Imię i nazwisko osoby wyrażającej zgodę:	
Data:	
Zapoznałam/zapoznałem się z Klauzulą Informacyjną Administratora danych i wyrażam zgodę na przetwarzanie danych osobowych mojego dziecka/podopiecznego w wyżej wymienionym celu i zakresie.	
Podpis osoby wyrażającej zgodę:	

Załącznik nr 24

WZÓR

REJESTR OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Nr upoważnienia	Imię i nazwisko	Data wystawienia upoważnienia	Od kiedy obowiązuje	Do kiedy obowiązuje	Uwagi

Załącznik nr 25

WZÓR

KLAUZULA POUFNOŚCI

W związku z działaniami prowadzonymi na terenie obiektów Centrum Integracji Społecznej w Świętochłowicach zobowiązuję się do:

1. Zachowania w tajemnicy wszelkich danych osobowych, do których mam dostęp w związku z wykonywaniem powierzonych czynności.

2. Zachowania w tajemnicy sposobów zabezpieczenia danych osobowych, do których mam dostęp w związku z wykonywaniem powierzonych czynności.

Odpowiedzialność określa art. 107 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, stanowiący:

1. Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony,

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.

2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej,

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech.

Powyższej tajemnicy zobowiązuję się dochować również po ustaniu zatrudnienia/współpracy.

Oświadczam, że zapoznałam/zapoznałem się z Klauzulą Informacyjną Administratora danych.

Imię i nazwisko:	
Data i miejsce:	
Podpis:	